Cassandra Crossing/ ED-209 ci aspetta dietro l'angolo

(136) — L'adozione di macchine per attività di sicurezza che dovrebbero svolgere gli umani non è solo pericoloso per questi ultimi…

Cassandra Crossing/ ED-209 ci aspetta dietro l'angolo

(136)—L'adozione di macchine per attività di sicurezza che dovrebbero svolgere gli umani non è solo pericoloso per questi ultimi, consente anche di trasferire alla macchina la responsabilità. Sta già accadendo.

10 ottobre 2008—Leggendo i giornali ed ascoltando i media capita di leggere articoli sulle future evoluzioni dei sistemi di sicurezza.

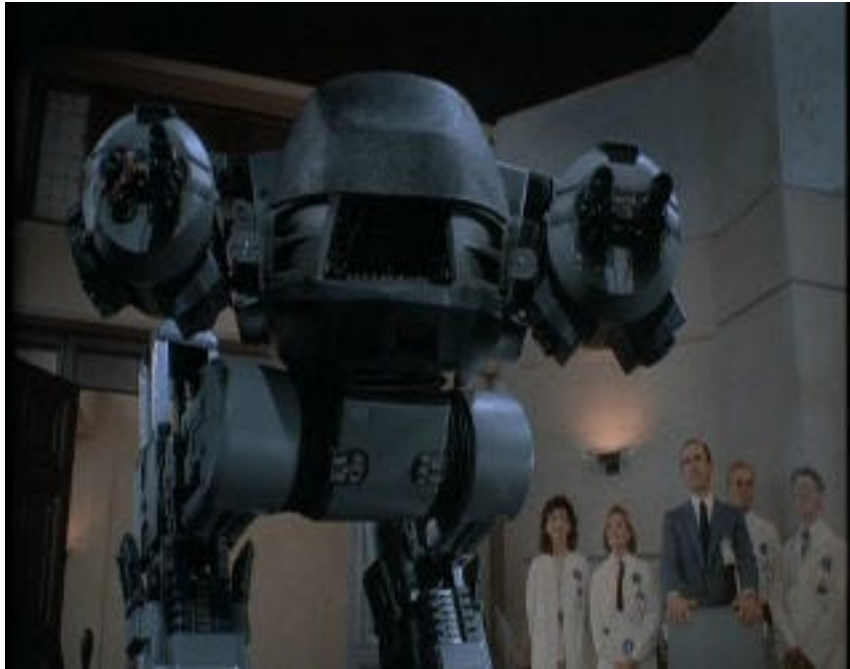
Mirabolanti algoritmi di riconoscimento facciale permettono già oggi di inseguire automaticamente un criminale in fuga tra le centinaia di telecamere della stazione Termini.

Database di informazioni sui passeggeri aerei permettono di scoprire potenziali terroristi prima che possano salire a bordo.

Algoritmi intelligenti permetteranno di distinguere espressioni e reazioni facciali di persone che mentono. L'analisi dei movimenti di ogni persona di una folla permetteranno di capire le intenzioni di un individuo particolare prima che compia azioni pericolose.

Tutto automatico, infallibile, economico, pulito.

La domanda che non riceve mai risposta, anzi che in questi articoli non viene nemmeno formulata, è se automatizzare operazioni così delicate possa essere, sia da un punto di vista di intelligence che legale e di tutela dei diritti civili, una cosa desiderabile?

Ci sono tre questioni importanti da considerare:

Affidabilità degli automatismi; non è il punto principale, ma avete presente quei piccoli problemi che affliggono gli automatismi che conoscete? La porta della banca che non vi fa entrare per via della fibbia della cintura? Serve per tenere fuori i mitra ed i loro proprietari, ma tiene fuori anche voi se non vi spogliate. Il bancomat che vi mangia una tessera perfettamente valida perché l'ha letta male?

E cosa dire delle risposte di certi impiegati allo sportello che ad una richiesta assolutamente normale rispondono che la procedura non glielo fa fare o che il computer si blocca? Affidereste la vostra vita ad uno di questi automatismi? Vi fareste giudicare da un giudice elettronico? Visitare da un medico elettronico? Confessare da un confessore elettronico?

Ci sono questioni che non ammettono automatismi.

Pattugliare una strada affollata e male illuminata, distinguere i buoni dai cattivi, farlo in maniera affidabile è già quasi impossibile per un essere umano. In "Robocop" di Paul Verhoeven il robot ED-209 (Enforcement Droid 209—Robot di costrizione) è una caricatura di questi automatismi per controllare le persone. Grosso e rumoroso, ruggisce come un leone ma funziona male, ammazza chi si arrende, si rivela forte ma totalmente inefficiente. Pero' è fabbricato da una multinazionale, è voluto da un politico locale, nasce per diventare una tecnologia militare…

Leggi, vincoli e regole: Lawrence Lessig dice, da avvocato ma in maniera molto efficace e corretta, che solo il software è legge nel cyberspazio. Dice questo

come parte della sua critica all'approccio del sistema legale americano che vuole normare la Rete considerandola un'ombra, un'analogia del mondo materiale.

E' assolutamente vero, poiché è di software che è fatto il cyberspazio, che senza di esso non esisterebbe neppure.

Nel nostro caso i termini del problema si rovesciano completamente. Può il software essere legge nel mondo materiale? Si dirà che un software non impone una legge, ma aiuta semplicemente gli umani a far rispettare le regole, creando vincoli che impediscono di delinquere o che rivelano potenziali delinquenti.

Qui si crea un circolo vizioso che rischia di portarci in posti pericolosissimi.

Le leggi nascono dal consenso per stabilire regole condivise; l'individuo decide liberamente se rispettarle oppure violarle e sopportarne le conseguenze. In ambedue i casi ci sono delle persone che devono valutare, eventualmente perseguire, giudicare, condannare.

E' il circolo virtuoso ma spesso dimenticato della democrazia e degli uomini liberi e dotati di libero arbitrio. Ma cosa succede se le regole si trasformano in vincoli? Se un meccanismo non umano come un software ti impedisce di violare una regola, se diventa un vincolo, una costrizione totale, un controllore supremo che decide automaticamente la colpevolezza?

L'esistenza di leggi e regole riconosce e fa salvo il libero arbitrio, l'esistenza di vincoli rende schiavi i giusti e gli ingiusti. Non è un dettaglio, è un completo stravolgimento, una antitesi.

Se avere leggi è cosa giusta, allora non si possono avere vincoli. I vincoli non hanno bisogno di leggi condivise, ed una volta istituiti possono diventare rapidamente e permanentemente strumenti di potere.

Purtroppo chi è disposto a rinunciare alla propria libertà in cambio di un briciolo di temporanea sicurezza non ha problemi a sottomettersi a vincoli piuttosto che dover rispettare, da uomo libero, leggi e regole condivise.

Uomini sulla catena di comando: tornando per un attimo ad ED-209 ho ancora in mente la situazione tragicomica in cui i tecnici che lo avevano avviato cercano disperatamente di fermarlo mentre sforacchia executive incravattati.

Non si tratta del solito archetipo della creatura che sfugge al suo creatore, e nemmeno del problema, pure questo attuale ma meno discusso, se robot autonomi abbiano o no il "diritto" di uccidere esseri umani. I droni volanti e le mitragliatrici autonome già lo possono fare e quindi la domanda e superflua.

Il problema è invece assai più a monte. E' ragionevole, nell'ambito di attività difficili, costose e complesse come quelle di intelligence, ritenere possibile l'automatizzazione del "riconoscimento dei sospetti"? E' lecito propagandare abbozzi di algoritmi tratteggiati in un paper universitario come la soluzione finale contro il terrorismo?

Non è questa la sede per ridicolizzare da un punto di vista tecnico o statistico questi algoritmi; chiediamoci semplicemente quanti veri terroristi sono stati identificati grazie ai dati personali dei passeggeri scambiati e memorizzati dal CAPPS-2? Quanti attentati sono stati sventati con l'uso della "no-fly list"?

Eppure un solo attentato sventato sarebbe uno scoop; invece le notizie che si leggono sulla stampa sono che Bill Clinton non è riuscito a salire sull'aereo o che in lista No-fly c'era un bambino di 4 anni.

Il problema è più insidioso. Immaginate che mentre state scegliendo lo yogurt che preferite al supermercato o vi provate un costume da bagno si accenda una luce rossa, ed un signore pieno di distintivi vi chieda di seguirlo. E' scattato il sistema automatico di rilevazione proattiva delle attività di taccheggio. Cosa fate? Vi arrabbiate? Vi lasciate perquisire tranquillamente tanto non avete niente da nascondere? Ed una volta identificati e riconosciuti innocenti chiederete che i dati di questo falso positivo vengano cancellati? Non potranno mai esserlo, non fosse altro per motivi di tutela legale di chi ha effettuato la perquisizione.

E se invece la luce rossa si accendesse mentre passate il check-in in aeroporto? Vi sentireste tranquilli perché c'è un umano nella catena di comando delle attività? Certo se trovaste un potente e benevolo saggio che riconoscesse subito la vostra specchiata onestà tutto bene. Ma le probabilità sono che invece vi capiti una persona annoiata e sottopagata, che vuole tornare a casa a fine turno e che sa perfettamente che nessuno è mai stato licenziato per aver dato retta alla luce rossa. In quel caso addio viaggio.

E vi va già bene perché la luce rossa l'hanno potuta vedere tutti, voi compreso, e che significava solo che non potevate volare. E se invece la luce rossa fosse nascosta e volesse dire che siete un sospetto terrorista? La targhetta sopra la luce rossa potrebbe indicare "gonfiore sospetto sotto il cappotto" mentre vi trovate nella metropolitana di Londra. Non mettetevi a correre per prendere il treno che sta partendo perché qualcuno, o magari qualcosa, potrebbe piantarvi le classiche sei pallottole in testa. E tante scuse alla famiglia: "Purtroppo la luce rossa si era accesa e lui ha cominciato a correre…".

Ovviamente sarà sempre previsto un essere umano nella catena di comando, ma la computerizzazione di attività di intelligence porterà inevitabilmente a trasferire autorità e fiducia dall'uomo alla macchina, dando quindi attendibilità a qualsiasi segnalazione, specie in condizioni di emergenza. Tanto a frittata fatta si potrà trasferire anche la responsabilità, la colpa, ad una patch mancante, ad un malvagio hacker, ad un filo staccato, ad un componente difettoso, ad un bug nel software.

Ricordate le traversie dell'ingegnere sospettato di essere Unabomber (vedi Cassandra Crossing/ Tu, Unabomber e la Data Retention)?

Gli investigatori avevano "calcolato", tramite l'uso di semplici database e di **una metodica aberrante**, che l'ingegnere apparteneva ad un gruppo di una dozzina di "colpevoli tecnicamente perfetti"?

Quanto è distante l'introduzione di automatismi nell'intelligence e nel controllo della popolazione dalla equazione "*Si è accesa la luce rossa e quindi sei colpevole*"?

Il motivo e la causa dell'accensione saranno probabilmente altrettanto inaccessibili dei motivi dell'indagine ne "*Il processo*" di Franz Kafka. Ovviamente per motivi di sicurezza!

Per gli errori, che non saranno chiamati "*morti ammazzati*" ma "*falsi positivi*", varrà poi il principio che è stato uno sfortunato incidente causato da un computer difettoso. O meglio, per ridurre ulteriormente i costi forse qualcuno riesumerà un loop legislativo "creativo" come quello che permetteva alle SS di giustiziare legalmente senza processo un nemico della patria, e che definiva nemico della patria chi veniva fucilato dalle SS.

Semplificazione e cost reduction da manuale, anche se a spese della libertà e della democrazia.

ED-209 vi fa ancora sorridere? O il pensiero dei suoi nipoti invisibili vi mette addosso una certa inquietudine? La vera inquietudine dovrebbe venir fuori già leggendo gli articoli di cui sopra, e dovrebbe spingervi a parlare ed esprimere la vostra opinione. Altrimenti dietro l'angolo, insieme ai nipoti di Ed-209, ci aspetterà lo storico e sempre in agguato slogan di "*Chi non ha niente da nascondere non ha niente da temere*".

Originally published at punto-informatico.it.

By Marco A. L. Calamari on August 28, 2017.

Canonical link

Exported from Medium on January 2, 2024.